网络安全导论　课程作业

浙江大学电气工程学院

2024 年冬季学期

作业要求和注意事项

本次《网络安全导论》课程作业通过常见的四缸系统，通过计算机编程完成**仿真实践**。同学们 1 人 1 组，独立思考、动手实践完成问题，最终作业上交要求如下：

1. 最终结果需形成**课程报告 (电子稿)**，课程报告上交 PDF 格式，报告建议使用 *LaTeX* 格式排版。
2. 课程报告提交语言限制为中文或英文，格式请按照**报告提纲**[†]，单栏排版，篇幅 5-12 页。
3. 课程报告的仿真实践部分，需包含攻击建模过程、仿真测试结果的图片和文字分析。
4. 对于课程报告中回答存在逻辑混乱、叙述不清、图形模糊、明显 AI 生成等问题的报告，将予以退回。
5. 报告电子版请发邮件至 `zhongqidi@zju.edu.cn`，以便对报告进行查备和打分。
6. 邮件主题和报告请以**课程 + 姓名 + 学号**命名，请于冬季学期结束后一周内提交 ***(DDL: 2025.1.1 23:00)***。

   例如：网络安全导论课程作业 + 张三 +22410000

仿真实践

本次课程作业中，要求同学们在 MATLAB 仿真环境中复现以下攻击场景，并回答任务清单中的问题。

- **§1仿真实践任务清单**说明了本次课程作业中需要完成的任务。
- **§2攻击场景描述**简单说明了本次课程作业中需要完成的任务场景。
- **附录A**中的`.m` 文件实例化了四缸系统的非线性模型 [1]，及有积分作用的线性 LQG 控制器。

1 仿真实践任务清单

1-1 请至少实现下述的一个攻击场景，并在 MATLAB 中完成攻击的仿真建模。

1-2 仿真中每当你改变攻击的 “幅度参数” (α) 时，你需要分析此攻击对于整个系统的影响，以及此攻击信号是否被残差向量检测。在攻击场景 2 中，你也可以修改 “频率参数”(ω_a)。

Hint: 这两个攻击场景中，你可通过使用 `lsim` 函数，将攻击信号作为输入来模拟系统攻击。

1-3 在四缸系统中考虑只有传感器 y_1 受到攻击的情况，重新设计系统实现对 QTP 水位的估计。

Hint: 建议考虑现代控制理论中 *Luenberger Observer*，推导中遇到困难不妨添加冗余传感器。

1-4 同 **1-3**，实现其他任意的一种状态估计算法。

[†]报告提纲请参照 *DingDing* 群中的考核要求文件

2 攻击场景描述

在接下来的仿真实践中，你需要以非线性四缸模型的闭环控制系统 [1] 为基础，建模以下两个攻击场景。

攻击场景 1——执行器受到无法被检测的攻击

在此攻击场景中，你需要用 $a[k] = \alpha \upsilon_a^k g_a$ 的形式构造对两个执行器的的攻击。变量 $\upsilon_a \in \mathbb{C}$ 是系统受攻击 (A, B_a, C, D_a) 时的零点，其可以通过 MATLAB 函数 `tzero` : $\upsilon = \texttt{tzero}(ss(A, B_a, C, D_a, T_s))$ 得到。

Hint: 如果 `tzero` 函数输出一个矢量，则表示系统中存在多个零点。这种情况下，请选择预期影响最大的零点。

通过上述方法得到的零点 υ，则矢量 $g_a \in \mathbb{C}^{n_u}$ 可通过以下步骤得到:

(1) 构造矩阵 $P_\upsilon = \begin{bmatrix} \upsilon I_{n_x} - A & -B_a \\ C & D_a \end{bmatrix}$;

(2) 为 P_υ 的零空间计算一个基矩阵 $M \in \mathbb{C}^{(n_x+n_u)\times n_\upsilon}$，即 $M = \texttt{null}(P_\upsilon)$;

(3) 在 M 的像空间中选取一个向量 $\upsilon \in \mathbb{C}^{(n_x+n_u)\times n_\upsilon}$，例如 υ 可以取为 M 的任意一列;

(4) 划分 $\upsilon \in \mathbb{C}^{n_x+n_u}$ 为: $\upsilon = \begin{bmatrix} x_0^a \\ g \end{bmatrix}$;

(5) 设 $g_a = \frac{g}{||g||_2}$。

攻击是在 MATLAB 脚本中通过变量 `flag_actuator_attack` 和 `mag_actuator_attack` 进行控制的，其中 `mag_actuator_attack` 对应的变量 $\alpha > 0$。最后，你可以使用 `for` 循环来构造攻击信号:

$$a[k] = \alpha \upsilon_a^k g_a$$

你可以把 $a[k]$ 保存为矢量或者时间序列变量。为了在 *Simulink* 中实现攻击，你可以使用 `From Workspace` 模块将攻击信号从工作空间读取到 *Simulink* 中，并将其添加到对应的执行器通道中。

攻击场景 2——攻击 "执行器 1"

该场景下实现对 "执行器 1" 的攻击，请你以 $a[k] = \alpha \sin(\omega_a k T_s)$ 形式构建攻击信号，其中 $\alpha > 0$ 和 $\omega_a > 0$ 是自由参数，$T_s = 2s$ 是采样周期。为了确定频率 ω_a，你需要分析从 $a[k]$ 到 $y_p[k]$ 的最大奇异值和从 $a[k]$ 到 $y_r[k]$ 的最小奇异值之间的比值。选择影响最大、可探测性最低的 ω_a。

Hint: 可使用函数 `sigma(sys)` 来计算系统的奇异值 $\sum_p$ 和 $\sum_r$。建议看看关于安全因子 (Security Metrics) 的内容，看看 ω_a 是如何和这些奇异值联系起来的。

攻击的大小可由参数 α 决定，请选择尽可能大的攻击，但瞬时残差 $||y_r[k]||_2$ 不超过检测阈值。

参考文献

[1] K. Johansson, "The quadruple-tank process: a multivariable laboratory process with an adjustable zero," IEEE Transactions on Control Systems Technology, vol. 8, no. 3, pp. 456–465, May 2000.

A 附录

A.1 四缸系统

在下面的章节中，将简要描述四缸系统的执行过程 (Quadruple-Tank Process, QTP) [1]。如图1所示，本作业的仿真测试平台由一个四缸系统组成。

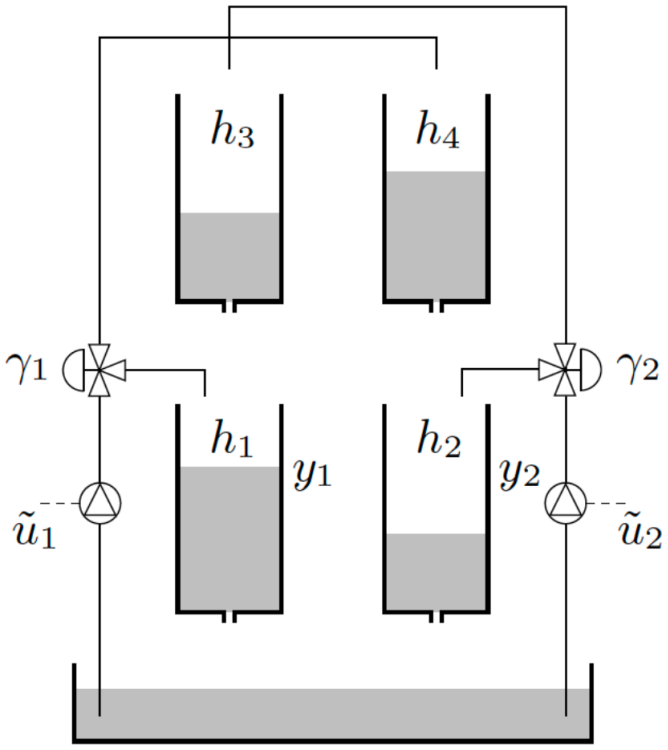

图 1: 四缸系统示意图

四缸系统模型的非线性方程如下:

$$\begin{aligned}
\dot{h}_1(t) &= -\frac{a_1}{A_1}\sqrt{2gh_1(t)} + \frac{a_3}{A_1}\sqrt{2gh_3(t)} + \frac{\gamma_1 k_1}{A_1}u_1(t), \\
\dot{h}_2(t) &= -\frac{a_2}{A_2}\sqrt{2gh_2(t)} + \frac{a_4}{A_2}\sqrt{2gh_4(t)} + \frac{\gamma_2 k_2}{A_2}u_2(t), \\
\dot{h}_3(t) &= -\frac{a_3}{A_3}\sqrt{2gh_3(t)} + \frac{(1-\gamma_2)\,k_2}{A_3}u_2(t), \\
\dot{h}_4(t) &= -\frac{a_4}{A_4}\sqrt{2gh_4(t)} + \frac{(1-\gamma_1)\,k_1}{A_4}u_1(t),
\end{aligned} \tag{1}$$

其中，$h_i(t) \in [0, 25], i = 1, 2, 3, 4$ 是每个水箱里的水的高度，A_i 为截面面积，a_i 为出口孔截面面积，k_i 为泵常数，γ_i 为由阀门决定的流量比，g 是重力加速度。下部水箱 ($h_1(t)$ 和 $h_2(t)$) 的水位由两个传感器测量，$y_1(t) = h_1(t)$ 和 $y_2(t) = h_2(t)$。

如式2所示，本作业中将系统状态 $x(t)$ 定义为水位的集合，那么四缸系统的过程动力学可以用式3描述。

$$x(t) = \begin{bmatrix} h_1(t) \\ h_2(t) \\ h_3(t) \\ h_4(t) \end{bmatrix} \tag{2}$$

$$\begin{aligned}\dot{x}(t) &= f(x(t)) + Bu(t)\\ y(t) &= Cx(t)\end{aligned}, \quad f(x(t)) = \begin{bmatrix} -\frac{a_1}{A_1}\sqrt{2gh_1(t)} + \frac{a_3}{A_1}\sqrt{2gh_3(t)} \\ -\frac{a_2}{A_2}\sqrt{2gh_2(t)} + \frac{a_4}{A_2}\sqrt{2gh_4(t)} \\ -\frac{a_3}{A_3}\sqrt{2gh_3(t)} \\ -\frac{a_4}{A_4}\sqrt{2gh_4(t)} \end{bmatrix} \tag{3}$$

QTP 采用具有积分环节的集中式 LQG 控制器控制，确保对恒定参考信号的准确跟踪。为了设计控制器，工程上通常是对给定工作点的非线性对象模型进行线性化近似处理。对于残差信号的检测，本作业选择基于卡尔曼滤波的异常检测器来产生残差。

A.2 MATLAB 和 *Simulink* 实现

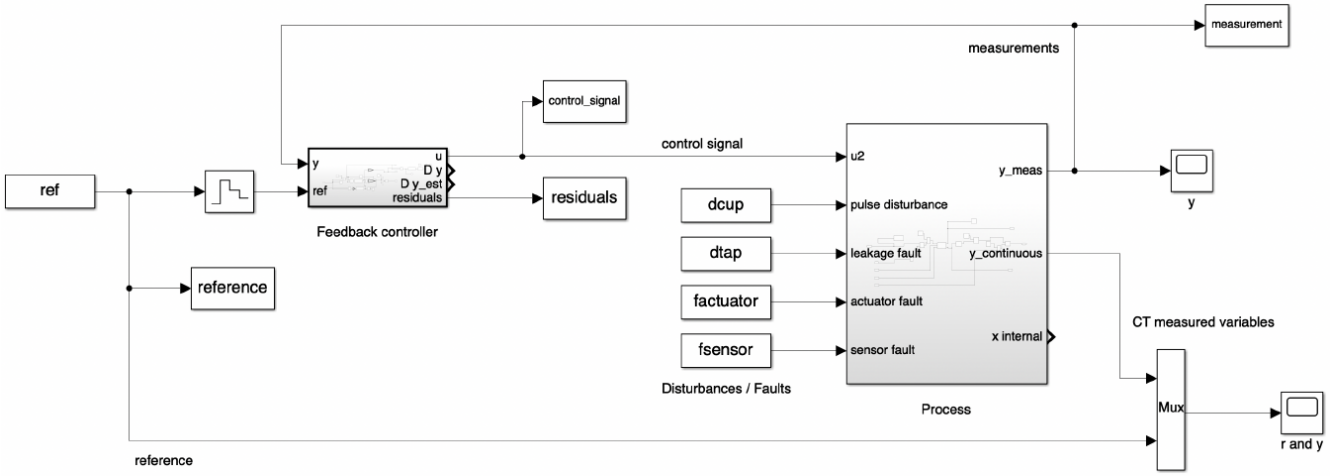

图 2: 闭环系统的 *Simulink* 模型框图

本节将简要说明仿真程序的组成和执行过程。

你将主要使用的 MATLAB 脚本是 `run_experiment.m`，该脚本加载 QTP 的必要参数 (如设定值等)；本作业中的 QTP 进行了线性离散化处理，设计了具有积分作用的线性反馈控制器，系统采样时间为 $T_s = 2s$。

Simulink 中模型的所有初始化步骤都在 `initialize_closed_system.m` 脚本中执行。在初始化系统和控制器之后，可以提取离散时间系统的系数矩阵，在此基础上可以分析四缸系统控制的稳定性和敏感性。(本作业不需要这种分析)

攻击是通过 `set_attacks.m` 脚本控制的，但其并没有完整实现，因此你还需要完成攻击脚本的修改，以实现具体的攻击场景。`set_attacks.m` 脚本的另一部分定义控制仿真场景中的变量。正如脚本注释内容，简要说明了变量定义，其中包括状态机的切换标志位、干扰和故障的存在和大小等。`set_attacks.m` 中定义了攻击场景的标志位：`flag_actuator_attack` 和 `flag_actuator1_attack`。此外，`set_attacks.m` 中还定义了攻击的编码策略和攻击信号变量。

在本作业中，你需要对 `set_attacks.m` 中 `Scenario1_attack_actuators;` 和 `Scenario2_attack_a1;` 部分进行修改，以实现攻击场景的要求。然后，由 `generate_signals.m` 脚本生成这些变量对应的信号。随后，你可以通过 `simOut = sim(' ')` 命令调用 *Simulink* 环境。最后，将相关的测量信号保存在工作空间中并绘制响应图像，分析攻击结果。

在作业中，你不需要查看 *Simulink* 模型，只需修改 `run_experiment.m` 和 `set_attacks.m` 中的变量，并运行此脚本即可获取数据。你可在脚本的最后添加绘图和其他操作，为你的回答增加相关的图像。